IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Criminal No. 1:19-cr-372
v.	)	
	)	
WILLIAM KINSEL,	)	
	)	
Defendant.	)	

STATEMENT OF FACTS

The United States and the defendant, WILLIAM KINSEL (hereinafter "KINSEL" or the "defendant"), agree that at trial, the United States would have proven the following facts beyond a reasonable doubt, with admissible and credible evidence:

1. From February 2019 through on or about May 24, 2019, KINSEL, a contractor or consultant of the United States, possessed documents or materials containing classified information of the United States by virtue of his contract or position, and did knowingly remove such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location, to wit: on an unauthorized media storage device within his workplace and on unauthorized media storage devices and other electronic devices within his home.

2. KINSEL maintained a Top Secret-Sensitive Compartmented Information (TS-SCI) security clearance allowing him to work on classified matters on behalf of the United States. KINSEL's most recent TS-SCI clearance was adjudicated in or around November 2017.

3. KINSEL completed refresher Cyber Training on October 4, 2018. KINSEL completed Annual Security Training on July 12, 2018. KINSEL received a refresher NATO

Security Briefing on August 2, 2018. KINSEL completed the annual Insider Threat Awareness Training on October 15, 2018. KINSEL signed a network User Acknowledgement Form on October 15, 2018, wherein he acknowledge he would "[p]rotect all media used on the system by properly classifying, labelling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide." KINSEL attended an "all hands" in-person security refresher training at COMPANY ONE on April 23, 2019. By virtue of his authorized security clearances and periodic training, KINSEL understood the proper procedures and restrictions for lawfully handling, retaining and securing classified documents or materials.

4. At all times material to the defendant's conduct, KINSEL worked as a subcontractor for COMPANY ONE, a properly cleared defense contractor. COMPANY ONE provided, among other services, cyber security support services to a branch of the United States military under a contract authorized and mandated by congress. KINSEL provided his services to COMPANY ONE under this authority. KINSEL performed his services as a subcontractor for COMPANY ONE within a classified secure space located in Stafford, Virginia, within the Eastern District of Virginia.

5. On May 9, 2019, a COMPANY ONE employee discovered a small Lexar Firefly thumb drive on the floor outside of a conference room located in the secured space within the office. A five person meeting–which KINSEL attended— had recently adjourned in the conference room. COMPANY ONE had neither distributed nor approved the use of the Lexar thumb drive storage device within the secured space. Only electronic devices (including thumb drives) explicitly approved by COMPANY ONE were permitted in this secure space.

6. The thumb drive was immediately submitted to COMPANY ONE's security unit and remained there unclaimed for approximately five days. On May 14, 2019, COMPANY

ONE security personnel inspected the contents of the thumb drive and discovered more than ten (10)[1] classified files marked "Secret" all relating to KINSEL's assigned project. This material was not authorized to be stored on the Lexar thumb drive. The thumb drive also contained non-work related files, including one file relating to a popular commercially distributed video game.

7. As part of the ensuing security investigation, the content on the Lexar thumb drive was compared with certain recent file activity on KINSEL's work-issued classified Secret Internet Protocol Router (SIPR) computer, which was issued to KINSEL by COMPANY ONE with a sterile hard drive. A folder on the Lexar thumb drive contained nine (9) files, at least three (3) classified as "Secret," which precisely matched a folder and its contents on the classified SIPR computer. The Lexar thumb drive "Secret" files were created on March 26, 2019, and modified on April 29, 2019. Additionally, COMPANY ONE personnel located an unauthorized writable CD on KINSEL's desk labeled "Traction." The unclassified Non-classified Internet Protocol Router (NIPR) laptop issued to KINSEL was found to contain a number of classified files, all related to KINSEL's assigned project. The unclassified laptops were not authorized to store classified data.

8. On May 17, 2019, some of the individuals assigned to the project who had attended the May 9, 2019, meeting, including KINSEL, were interviewed about a possible "spillage" of classified information. KINSEL made false statements during this interview, including that he had never brought any unauthorized electronic or media storage devices, including hard drives, CDs, and thumb drives into the workplace secured area. KINSEL stated the only unauthorized device he brought into the secured workspace was a fitness watch, which he immediately removed upon discovering he had carried the watch into the secured space.

[1] Including duplicates and/or additional drafts of the same document or substantially same document, approximately eighty-five (85) classified files were located on this thumb drive.

KINSEL also stated that he had never downloaded classified material onto any unclassified or unauthorized devices, and that he was not authorized to remove classified data from the COMPANY ONE facility.

9. On May 21, 2018, KINSEL and other employees were again interviewed about the "spillage" incident. KINSEL stated that he was not permitted to conduct classified work or store classified data on work-issued unclassified laptops.

10. KINSEL was interviewed again on May 24, 2019. KINSEL admitted that his prior statements on May 17, 2019, were false. KINSEL admitted that, contrary to what he stated in the previous interviews, he had in fact brought classified data home with him. Additionally, the Lexar Firefly thumb drive that was discovered in the secure area on May 9, 2019, belonged to him and must have accidently fallen out of his pocket after he exited the meeting that day.

11. KINSEL explained that, when in the secured space at COMPANY ONE, he would transfer the classified files to the Lexar thumb drive, which he would bring home with him at the end of his work day. Once home, KINSEL would transfer the files from the Lexar thumb drive to a personal computer in his basement, which he would then use to store and work on both classified and personal files at home during non-work hours. Once done working on the files, KINSEL would move the classified data to his external hard drive for storage at home, erase the files from his personal computer, and then bring the finished product back to COMPANY ONE using the Lexar thumb drive. KINSEL would sometimes rename the classified files and their parent folders in an attempt to avoid detection from COMPANY ONE personnel.

12. KINSEL stated COMPANY ONE never authorized him to remove classified material from the secure space or to take such material off-site for any reason. KINSEL knew

what he was doing was wrong, but brought classified materials home so he could save time and continue to work on his assignments after hours.

13. Following the interview, KINSEL consented to a search of the basement area of his home for the purpose of recovering the unauthorized classified files that he had removed from COMPANY ONE. KINSEL surrendered the following electronic devices, which he stated might potentially contain classified material: (a) a Western Digital MyBook external hard drive (serial number WX6ID6574COF); (b) a yellow thumb drive (no serial number); (c) a Data Stick Pro 8 gigabyte thumb drive (no serial number); (d) a Gorilla thumb drive (no serial number); (e) a Bechtel thumb drive (no serial number); and (f) a Lenovo laptop (serial number DFO1H4L3). Subsequent review of the aforementioned electronic devices revealed that the Western Digital MyBook external hard drive contained numerous documents (including duplicate or near-duplicate files) relating to KINSEL's assigned project and internally classified as "Secret." These files were included comingled on the device with thousands of KINSEL's personal files, including, but not limited to, torrent files, emails, music, Word documents, and other files. Similarly, numerous "Secret" files relating to KINSEL's assigned project were also located on the Lenovo laptop and as well as the Data Stick.

14. KINSEL unlawfully removed and retained hundreds of documents classified as "Secret" relating to the work he performed on behalf of the United States. A number of these documents were repeat versions or working drafts of earlier documents.

15. This statement of facts includes those facts necessary to support the plea agreement between KINSEL and the United States. It does not include each and every fact known to KINSEL or to the United States, and it is not intended to be a full enumeration of all of the facts surrounding KINSEL's case.

16. Pursuant to paragraph 14 of the Plea Agreement, this statement of facts shall be admissible as a knowing and voluntary confession in any proceeding against KINSEL upon a breach by him of the plea agreement. Moreover, KINSEL waives any rights that he may have under Fed. R. Crim. P. 11(f), Fed. R. Evid. 410, the United States Constitution, and any federal statute or rule in objecting to the admissibility of the statement of facts in any such proceeding.

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

By: _____
Dennis M. Fitzpatrick
Assistant United States Attorney

Defendant's Signature: After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, William Kinsel, and the United States, I hereby stipulate that the above statement of facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 12-11-19
12-19-19

_____
William Kinsel
Defendant

Defense Counsel Signature: I am counsel for the defendant in this case. I have carefully reviewed the above statement of facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 12-11-19
12-09-19 KPT

_____
Kenneth P. Troccoli, Esq.
Counsel for Defendant